

18-1241-ADC

18-1244-ADC

AFFIDAVIT

I, Patrick T. Winn being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the search for the following items:

- a. ZTE cell phone, S/N: 32FB76120283, black in color
- b. BLU cellphone, model #R0031UU, s/n: 164050016017003944
- c. iPhone, model #A1453, IMEI #352028065759255
- d. iPhone 8, black in color
- e. Tagged Account: 6031308765
- f. Facebook Account : ricky.rude.161
- g. Yahoo email account: ryandinero123@yahoo.com

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since September 2003. I am currently assigned to the FBI's Maryland Child Exploitation Task Force where I predominately investigate child sex trafficking and violent crimes against children. I have previously been assigned as a Supervisory Special Agent at FBI Headquarters' Asset Forfeiture/Money Laundering Unit as well as a Special Agent in the San Diego Division where I worked complex white collar crime matters and online sexual exploitation of children matters for six years. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes as well as the investigation of various child exploitation crimes. During the more than fourteen years in Federal law enforcement, I have

FILED
LOGGED
MAY 11 2018
ENTERED
RECEIVED
by CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND
DEPUTY
CRS

been involved in investigations of sexual exploitation of children to include child pornography, enticement of minors and child sex trafficking.

IDENTIFICATION OF THE ITEMS TO BE EXAMINED

3. The black ZTE cell phone, serial number 32FB76120283 is in the custody of the Maryland State Police and is described in Attachment A-1 (hereafter the "VICTIM PHONE #1")

4. The BLU cell phone, model #R0031UU, serial #164050016017003944, is in the custody of the FBI and is described in Attachment A-1 (hereafter the "VICTIM PHONE #2").

5. The iPhone cell phone, model A1453, IMEI #352028065759255, is in the custody of the FBI and is described in Attachment A-1 (hereafter the "VICTIM PHONE #3").

6. The black iPhone 8 cell phone, with a cracked screen protector, is in the custody of the Maryland State Police and is described in Attachment A-1 (hereafter the "SUBJECT PHONE")

7. The Tagged account 6031308765, as further described in Attachment A-2 (hereinafter the "TARGET TAGGED ACCOUNT"), the records of which are stored at premises owned, maintained, controlled or operated by The Meet Group, who's offices are located at 100 Union Square Drive, New Hope, Pennsylvania, 18983.

8. The Facebook Account ID "ricky.rude.161", as further described in Attachment A-3 (hereinafter the "TARGET FACEBOOK ACCOUNT"), the records of which are stored at premises owned, maintained, controlled or operated by Facebook with offices located at 1601 Willow Road, Menlo Park, California, 94025.

9. The Oath Holdings, Inc. (Yahoo) email account ryandinero123@yahoo.com as further described in Attachment A-4, (hereafter the "TARGET YAHOO ACCOUNT"), the records of which are stored at premises owned, maintained, controlled or operated by Oath Holdings, Inc. with offices located at 701 First Ave., Sunnyvale, California, 94089.

10. The applied for warrants would authorize examination of the contents and records associated with the above listed subject cell phones, email accounts and social media accounts for the purpose of identifying electronically stored data particularly described in Attachment B-1, B-2, B-3 and B-4 to this affidavit. I make this affidavit in support of an application for warrants to search these electronic devices and electronic communication accounts.

11. Based on the information outlined below, I believe that RYAN PARKS, YASMINE JAMES and others conspired to cause at least three juvenile females and others to engage in prostitution. Based upon the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 1591 (Sex Trafficking of Children or By Force, Fraud, or Coercion), Title 18, United States Code, Section 1594 (Conspiracy to Commit Sex Trafficking), Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) and Title 18, United States Code, Section 2252 (Sexual Exploitation of Minors), have been committed and were facilitated by the user of the subject cell phones and electronic communication accounts and that evidence of those crimes will be found in the subject cell phones and subject electronic communication accounts.

12. The information contained in this Affidavit is based upon my personal knowledge, as well as on information and documents made available to me by other law enforcement officers and witnesses. Since this Affidavit is being submitted for the limited purpose of securing search warrants, I have included only those facts that I believe are sufficient to establish probable cause to believe that PARKS, JAMES and others have violated 18 U.S.C. §§ 1951, 1954, 2252A(a)(5)(B), 2252 and that evidence, fruits and instrumentalities of those violations will be found within the subject electronic devices and electronic communication accounts.

PROBABLE CAUSE

13. On November 21, 2017, Maryland State Police Corporal Chris Heid and Baltimore County Police Detective Chad Lettau responded to the Knights Inn, located at 6700 Security Boulevard, Baltimore, Maryland in search of a missing 15 year old female, hereafter referred to as VICTIM #1. VICTIM #1 was recovered outside the hotel and placed in a juvenile facility.

14. Following her recovery, VICTIM #1 disclosed that she was involved in human trafficking while staying at the Knights Inn. As a result, she was forensically interviewed by a Baltimore County social worker. During the interview VICTIM #1 explained that she met subject RYAN PARKS through the internet on the social media site, Tagged.com. PARKS introduced himself as "Dinero" and VICTIM #1 introduced herself as "Sasha." VICTIM #1 had a suspicion that PARKS was a pimp based on the comments and pictures she observed on his Tagged profile. After indicating that she "liked" one of the pictures on his profile, PARKS sent a message to VICTIM #1 asking her if she wanted to make some money. PARKS sent an Uber to pick up VICTIM #1 and bring her to his house. Once at the house, PARKS and VICTIM #1 smoked marijuana and had sex. VICTIM #1 told PARKS she was 17 years old and was in foster care.

15. PARKS discussed with VICTIM #1 about making money through prostitution and posting ads on the internet website Backpage.com. PARKS used his iPhone cell phone (SUBJECT PHONE) to create an ad on Backpage for VICTIM #1. PARKS took pictures of her with his phone for the ad. Once the ad was posted on Backpage, several of the pictures were deleted from the posting by Backpage because they contained nude images of VICTIM #1. PARKS used the VICTIM #1 PHONE to download a "text me" app and create a new phone

number she could use to communicate with potential prostitution customers. PARKS instructed VICTIM #1 on how to make dates with customers and what to say to them. PARKS provided VICTIM #1 with the rates she was to charge each customer, which included \$80 for a short stay, \$100 for 20 minutes, \$120 for a half hour and \$180 for one hour. PARKS told VICTIM #1 to use condoms with each customer and provided her with several Magnum brand condoms.

16. PARKS told VICTIM #1 to collect the money from each customer before the date started and to check the money to make sure it was real. Once the customer was in the room and she had the money, PARKS instructed VICTIM #1 to text him "G" to the SUBJECT PHONE from the VICTIM PHONE #1. This "G" was a signal that VICTIM #1 was to convey to PARKS that she was ok and the date would proceed. In the beginning, PARKS took most of the money VICTIM #1 earned from the prostitution dates and only gave her \$20 from each date. After being confronted by VICTIM #1, PARKS agreed to give the majority of money earned from each date to VICTIM #1. VICTIM #1 estimated that she saw no more than 10 customers.

17. Some of the money that PARKS gave VICTIM #1 was for her to pay for the hotel room they were in. Records obtained from the Knights Inn showed that a NORRIS POWELL rented room #316 where VICTIM #1 was staying. A clerk at the Knights Inn recognized PARKS' picture and knew him to rent numerous rooms in the past. However, he was later placed on a 'do not rent' list and had POWELL rented the room for him instead.

18. On the second day, VICTIM #1 met a woman she knew as "Star" and has since been identified as YASMINE JAMES. JAMES was PARKS's friend and on the day JAMES arrived, she was with another female who also appeared to be learning how to make prostitution dates as well.

19. On December 18, 2017, a Baltimore County District Court Commissioner issued an arrest warrant for PARKS on charges of Human Trafficking, Third Degree Sex Offense and various prostitution charges. On January 10, 2018 PARKS was arrested by the Maryland State Police while meeting with his Probation Officer. At the time of his arrest, PARKS had a cell phone on his person which is identified as the SUBJECT CELL PHONE. This phone was seized and placed into evidence by the Maryland State Police. During a post-Miranda interview, PARKS stated that he met VICTIM #1 through Tagged.com and arranged for her to come to his house. The two discussed prostitution and shortly thereafter got a room at the Knights Inn. PARKS had someone else rent the room but claimed he had just met the man in the parking lot. PARKS helped VICTIM #1 create an ad on Backpage.com and helped her set the rates. PARKS used the SUBJECT PHONE to take pictures of VICTIM #1 and also has pictures of other women he has posted ads for in the past. PARKS used the SUBJECT EMAIL ACCOUNT to post the ads, ryandinero123@yahoo.com, and he stated that he agreed to only take \$20 per date for his work as her security guard.

20. PARKS stated that he and JAMES also worked with other women who were engaging in prostitution. PARKS posted their ads on Backpage.com and took pictures of them as well. PARKS provided the women with condoms and told the woman that he collected money from them so they would not get robbed. In the interview, PARKS denied being a pimp but instead described himself as a security guard. When asked how old PARKS believed VICTIM #1 was, he replied that he thought she was 17.

21. On 1/26/2018, Corporal Heid interviewed YASMINE JAMES who was in the custody of Baltimore County Department of Corrections. JAMES identified PARKS as her boyfriend and described him as a pimp that had many females working for him. JAMES

observed PARKS creating and posting ads for the women. JAMES recalled meeting VICTIM #1, who told her in front of PARKS that she was 17 and a run-away from a foster home. According to JAMES, PARKS runs everything and takes all of the money from the women. During each of the dates, PARKS leaves the room but stays close by until the prostitution customer leaves. JAMES had cautioned VICTIM #1 that if she stayed around that PARKS would eventually begin assaulting her. JAMES was able to identify other women that worked for PARKS through a review of the subpoenaed Backpage ads.

22. On November 28, 2017, your Affiant issued a subpoena to Backpage.com for the telephone number 443-470-5880 and email account ryandinero123@yahoo.com. Backpage provided their results electronically which consisted of four files. Contained in these four files were 268 Backpage ads covering the time frame of February 25, 2017 to November 23, 2017. The email address associated with all of these ads is ryandinero123@yahoo.com. I know through my experience investigating this violation, that each time a user posts a new ad on Backpage.com or renews an existing ad, Backpage.com will send an email to the user's email address confirming the posting.

23. Through a review of these ads, eight of them posted in November 2017 depict VICTIM #1. The ad contained three pictures of VICTIM #1, in which she is lying or sitting on a bed and only wearing a bra and underwear. In addition, there are four images of what appears to be VICTIM #1 in which her bare buttocks are exposed. However, these four images were removed from the original ad posting by Backpage because they contained nudity.

VICTIM PHONE #1

24. Following the recovery of VICTIM #1, the phone she used to arrange prostitution dates, communicate with PARKS and access her Tagged.com account was recovered by

Corporal Heid. Through a Baltimore County District Court, a search warrant was authorized to search this phone on 11/28/2017. Although the contents of the phone was extracted, a thorough analysis was not completed by investigators. Detective Lettau, however, did observe several text messages between PARKS and VICTIM #1 and observed pictures of VICTIM #1 that were used in her Backpage ads.

FACEBOOK ACCOUNT

25. During one of the initial meetings with VICTIM #1, she was only able to provide law enforcement with a physical description of PARKS, his street name of "Dinero" and his social media accounts that she used to communicate with him. These accounts included the TARGET TAGGED ACCOUNT as well as the TARGET FACEBOOK ACCOUNT. At the time, the TARGET FACEBOOK ACCOUNT was publicly available to view. VICTIM #1 showed Corporal Heid the location of the page and positively identified PARKS as the man in one of the pictures on the profile. Through a review of these publicly available pictures, Corporal Heid observed an image of money on a counter. In the corner of the picture was a Maryland learners permit. After zooming in on the license, Corporal Heid was able to read the name as Ryan Russel PARKS, with a date of birth of 10/27/1992 and identification number of P-620-755-751-827. Through a search of the Maryland Motor Vehicle Administration records on 4/19/2018, this same identification number is confirmed to be assigned to PARKS.

26. In addition to the picture described above, Corporal Heid also observed a picture of PARKS. In the comment section below the picture, YASMINE JAMES "tagged" the photo of PARKS with the comment "Daddy". Based on my training and experience, I know that subjects of Human Trafficking investigations have their victims, or women working as prostitutes for them, refer to them as "Daddy".

27. On December 18, 2017, Corporal Heid issued a preservation request to Facebook to preserve all of the records relating to the TARGET FACEBOOK ACCOUNT. Following the initial 90 day retention period, Corporal Heid requested an extension to the initial 90 day preservation.

28. Facebook is a free social networking website that provides a host of services to its users. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. Facebook users can post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. A particular user’s profile page includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links.

29. Facebook has a Photos application, where users can upload images and videos. Another feature of the Photos application is the ability to “tag” (i.e., label) other Facebook users in a photo or video. For Facebook’s purposes, a user’s “Photoprint” includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

30. Facebook users can exchange private messages with one another. These messages, which are similar to email messages, are sent to the recipient’s “Inbox” on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

31. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger. The Facebook Gifts feature allows users to

send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook also has a Marketplace feature, which allows users to post free classified ads, including items for sale, housing, jobs, and the like.

TAGGED ACCOUNT

32. Upon VICTIM #1’s recovery, she provided investigators with a screen shot of her Tagged.com account and that for PARKS which she used to meet and communicate with him (TARGET TAGGED ACCOUNT). PARKS’s account user name contained a combination of letters and emoticons or pictures. The screen name appeared to be a capital letter “D”, an image of a stack of money with wings, two images of a stack of money, and two images of a brown bag with a dollar sign on it. The user’s age was listed as 25 years old and their location was Gwynn Oak, Maryland. In addition, there is a picture of a black male resembling PARKS wearing a black hat and red pants.

33. On March 6, 2018, your Affiant issued a subpoena to Tagged.com via The Meet Group Legal Team. Without the ability to type the exact screen name to Tagged in the subpoena due to the emoticons, Tagged was provided with the TARGET YAHOO ACCOUNT, ryandinero123@yahoo.com. Based on this email account, Tagged.com provided their response on March 16, 2018 identifying the TARGET TAGGED ACCOUNT number as 6031308765. The user name associated with this account was “Dinero Parks” with a date of birth of October 27, 1992 and provided their town as Gwynn Oak, Maryland. Note that this is true date of birth for PARKS. The email address associated with the account was ryandinero123@yahoo.com.

34. In addition, Tagged.com provided historical Internet Protocol (IP) Address logs for the TARGET TAGGED ACCOUNT. On November 16, 2017, the TARGET TAGGED

ACCOUNT was accessed from IP address 174.205.3.100. Through a review of the Backpage.com ads for VICTIM #1 on November 16, 2017, one ad (Post ID# 28320417) was posted from the same IP address, 174.205.3.100.

35. On March 19, 2018, your Affiant issued a preservation request to Tagged.com to preserve any and all records relating to the TARGET TAGGED ACCOUNT.

VICTIM PHONES #2 & #3

36. In January 2018, Fairfax County Police Department had a reported missing 17 year old juvenile female (VICTIM #2) who was eventually located and recovered at a Knights Inn hotel in Baltimore County Maryland. VICTIM #2 disclosed to Fairfax County Police Detective Sean Craddock that when she ran away, she would travel to Baltimore for a couple weeks at a time. VICTIM #2 disclosed to Detective Craddock that she was involved in prostitution in the Baltimore area each time she left her home.

37. Upon return to her home in January 2018, VICTIM #2 had three phones on her person; 1) her personal phone, 2) a phone she used to make prostitution dates and 3) a phone used by another female who also worked with PARKS. On 1/26/2018, Detective Craddock obtained written consent from VICTIM #2's mother to search the second and third phones in Victim #2's possession. Pursuant to that consent, Detective Craddock attempted to review the contents of the two phones. He was able to open and review the contents of VICTIM PHONE #2, and he observed messages from apparent prostitution customers asking VICTIM #2 questions about how long they would stay, how much they would pay and what sex acts they wished to have performed. Detective Craddock also told me that VICTIM PHONE #2 contained photographs of VICTIM #2 used in her Backpage ads.

38. Although Detective Craddock received consent to review the third phone in VICTIM #2's possession (VICTIM PHONE #3), he was unable to review the contents because VICTIM PHONE #3 was locked and was unable to be accessed by Detective Craddock. The circumstances surrounding the recovery of Victim #2 from the Knights Inn hotel in Woodlawn, Maryland, involved police being called to the hotel because of a possible domestic dispute. Upon arrival, law enforcement observed VICTIM #2 running away from a hotel room. VICTIM #2 would not disclose what had happened to her, but she told police that she had been in a room with an 18 year old female and an unknown male. Based on the facts reported by Baltimore County Police, VICTIM PHONE #3 is believed to belong to the female who was staying in the Knights Inn hotel room with VICTIM #2. VICTIM #2 told Detective Craddock that VICTIM PHONE #3 was used by a female involved in prostitution with PARKS at the Knights Inn hotel.

39. On February 5, 2018, Corporal Heid and your Affiant interviewed VICTIM #2 in Virginia. VICTIM #2 disclosed that she became involved in prostitution at the direction of PARKS. VICTIM #2 would stay with PARKS in hotels in Baltimore making prostitution dates for a couple of weeks and then return home. PARKS rented the hotel rooms at several identified hotels in Baltimore with VICTIM #2 and that she would see prostitution customers in these rooms. PARKS dictated the rates VICTIM #2 charged each customer and PARKS received \$20 from each date VICTIM #2 made for providing security for her. PARKS later took all of VICTIM #2's money she earned through prostitution.

40. PARKS provided VICTIM #2 with a phone to use to make the dates. PARKS got upset with VICTIM #2 because she took the phone with her when she left him.

41. On April 23, 2018, your Affiant interviewed YASMINE JAMES. JAMES stated that she was asked by PARKS to teach VICTIM #1 and VICTIM #2 how to make prostitution

dates and how to communicate with the customers. In exchange for training them, PARKS agreed to pay JAMES a portion of the proceeds from each date completed by VICTIM #1 and VICTIM #2.

SUMMARY

42. Your Affiant knows through his knowledge, training and experience that subjects and victims will use cellular phones and electronic communication accounts during the commission of these crimes to communicate to any subjects assisting in the criminal act. Those involved in trafficking will also record photographs and videos of the victims of Human Trafficking using their cell phones and keep records or trophies of the criminal acts on the cellular phones. The traffickers will many times transfer their cell phone data to computers and social networking sites to display their work to attract attention from admirers.

43. Your Affiant knows that individuals involved in human trafficking, to include Human Traffickers and the victims of human trafficking, utilize iPods, tablets and cell phones which can be connected wirelessly to the Internet. These devices are used to send and receive emails, search and post prostitution advertisements, communicate with customers through telephone calls and text messages, communicate with their traffickers, download texting applications (apps) and take pictures or videos of the victims and traffickers.

44. The communications victims of human trafficking have with customers occur both through telephone calls, over text messaging applications, through social meeting applications and email communications. These communications include discussions about when and where to meet, how much the customer will pay for time with the victim as well as what sex acts will occur when they meet. The victims will also communicate with their traffickers to let them know when a customer is coming, how much he is paying, when the customer is done so the

trafficker can return to the room, making arrangements to rent and pay for hotel rooms, posting prostitution ads on the Internet and addressing the victims personal needs such as meals, hygiene products and drugs or cigarettes.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

45. I anticipate executing the warrant on the subject cell phone devices currently in the possession of the FBI and Maryland State Police which should contain copies of records and other information (including the content of communications) particularly described in Section I of Attachment B-1 of the warrant. I also anticipate executing the warrant on the target email account, target Tagged account and target Facebook account currently in the possession of Yahoo! Inc and parent company Oath Holdings, Inc., Tagged.com and Facebook, respectively, which should contain copies of records and other information (including the content of communications) particularly described in Section I of Attachments B-2, B-3 and B-4 of the warrant respectively. Upon receipt of the information described in Section I of Attachment B1, B-2, B-3 and B-4, government-authorized persons will review that information to locate the items described in Section II of Attachment B1, B-2, B-3 and B-4.


CONCLUSION

46. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe on the subject electronic devices, electronic communication accounts and social media accounts there exists evidence of a crime, contraband and/or fruits of a crime. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that the subject cell phones, target e-mail account, target Tagged account and target Facebook account listed in paragraph 1, above, contains evidence of violations of Title 18, United States Code, Section 1591 (Sex Trafficking of Children or By Force, Fraud, or Coercion),

Title 18, United States Code, Section 1594 (Conspiracy to Commit Sex Trafficking), Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) and Title 18, United States Code, Section 2252 (Sexual Exploitation of Minors). Accordingly, search warrants are requested.

47. This Court has jurisdiction to issue the requested warrants to search records on the subject devices in possession of the Federal Bureau of Investigation because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. § 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a “district court of the United States that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(I).

Respectfully Submitted,


Patrick T. Winn Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on April 26, 2018


A. David Copperthite
United States Magistrate Judge

ATTACHMENT A-1

ITEMS TO BE SEARCHED

(Phones)

The following items were seized and are currently in the custody of the Federal Bureau of Investigation and Maryland State Police:

- A black ZTE cell phone, serial number 32FB76120283, in the custody of the Maryland State Police (“VICTIM PHONE #1”);
- A BLU cell phone, model #R003IUU, serial #164050016017003944, in the custody of the FBI (“VICTIM PHONE #2”);
- An iPhone cell phone, model A1453, IMEI #352028065759255, in the custody of the FBI (“VICTIM PHONE #3”); and
- A black iPhone 8 cell phone, with a cracked screen protector, in the custody of the Maryland State Police (“SUBJECT PHONE”)

ATTACHMENT B-1

Information to be Seized by Law Enforcement Personnel

(Phones)

All information, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 1591 (Sex Trafficking of Children or By Force, Fraud, or Coercion), Title 18, United States Code, Section 1594 (Conspiracy to Commit Sex Trafficking), Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) and Title 18, United States Code, Section 2252 (Sexual Exploitation of Minors), including information pertaining to the following matters, including attempting and conspiring to engage in the following matters (the terms “records” and “information” include all of the below items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form):

1. Records relating to the purchase or placement of advertisements for commercial sex;
2. Records relating to the purchase or use of stored value cards, gift cards, and other financial instruments which may be used to purchase advertisements for commercial sex;
3. Records relating to the solicitation of customers for commercial sex;
4. Records relating to the scheduling of appointments for commercial sex;
5. Records relating to the travel or transportation of individuals to engage in commercial sex;
6. Records relating to sexually explicit or suggestive images of minors that may be used in furtherance of commercial sex trafficking;
7. Records relating to the recruitment, enticement, solicitation or coercion of individuals to engage in commercial sex;
8. Records relating to the fruits or instrumentalities of commercial sex trafficking, including currency and other financial instruments, jewelry, vehicles, controlled substances, and firearms.
9. Records relating to the kidnapping or attempts to escape from kidnapping of any individual.
10. Credit card and other financial information including but not limited to bills and payment records;
11. Evidence of who used, owned, or controlled the device listed on Attachment A-1;
12. Passwords and encryption keys, and other access information that may be necessary to access the device listed on Attachment A-1 and other associated accounts accessed using the device.
13. Any and all communications to include, but not limited to SMS messages, MMS messages, texting applications, notes and email communications with PARKS, JAMES,

Victim #1, Victim #2 and other known and unknown witnesses, victims or co-conspirators.

14. Subscriber Information, including the name and location, supplied by the user at the time of registration, the date the device was activated and all of the services of the device.
15. Records of user activity for each connection made to or from the Target device, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses, and any telephone, instrument or other unique identifiers;
16. All information about each communication sent or received by the device, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, telephone numbers and texting application numbers);
17. The contents of all e-mails stored in the account, including copies of e-mails sent to and from the device, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
18. The contents of all SMS and/or MMS text messages stored in the device, including copies of messages sent to and from the device, draft messages, the source and destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message;
19. Any deleted emails or messages, including any deleted information described in Paragraphs 17 and 18 above;
20. All Internet history and Internet search records, including the specific terms searched in association with the Target device, the dates, times and time zones of all searches, the IP addresses or telephone or instrument identifying numbers associated with those searches, and any data related to the results of the searches associated with the Target device and the Target device's use of any search results;
21. All records or other information regarding the identification of the device, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of services utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, and account status;
22. All records or other information stored by an individual using the device, including address books, contact and buddy lists, calendar data, pictures, videos and other data files;
23. All telephone or instrument numbers associated with the Target device (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services

Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”));

24. Pictures and videos depicting PARKS, JAMES, Victim #1, Victim #2 or other known and unknown witnesses, victims or co-conspirators.
25. Any and all phone contacts, to include phone numbers, physical addresses and email accounts.
26. Saved location information where pictures, videos and locations searches were conducted.

ATTACHMENT A-2

DESCRIPTION OF LOCATION TO BE SEARCHED

(Tagged Account)

This warrant applies to information associated with the Tagged.com account:

6031308765

which is stored at premises owned, maintained, controlled, or operated by The Meet Group, 100 Union Square Drive, New Hope, Pennsylvania, 18983.

ATTACHMENT B-2

PARTICULAR THINGS TO BE SEIZED

(Tagged Account)

I. Information to be disclosed

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Tagged.com (the "Target ISP"), the Target ISP is required to disclose the following information to the government for the accounts or identifiers listed in Attachment A-2 (the "Target Account"). Such information should include the below-described content of the subject account:

- a. Subscriber Information, including the name and location, supplied by the user at the time of registration, the date the account was created and all of the services of the Target ISP used by each Target Account.
- b. Records of user activity for each connection made to or from the Target Accounts, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses, and any telephone, instrument or other unique identifiers collected by the Target ISP and associated with the Target Accounts;
- c. All information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);
- d. The contents of all communications stored in the account, including copies of messages sent to and from the account, draft messages, the source and destination addresses associated with each messages, the date and time at which each message was sent, and the size and length of each message;
- e. Any deleted messages, including any deleted information described in subparagraph "d," above;
- f. All internet search records, including the specific terms searched in association with the Target Account, the dates, times and time zones of all searches, the IP addresses or

telephone or instrument identifying numbers associated with those searches, and any data related to the results of the searches associated with the Target Account and the Target Account's use of any search results;

- g. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of services utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- h. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, videos and other data files;
- i. All local and long distance telephone connection records;
- j. All telephone or instrument numbers associated with the Target Account (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"));
- k. All wire and electronic communications held or maintained by the Target ISP at any time in association with telephone communication services, including but not limited to text or SMS messaging and stored audio communications, for the use of or associated with the Target Account; and
- l. All records pertaining to communications between the Target ISP and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 1591 (Sex Trafficking of Children or By Force, Fraud, or Coercion), Title 18, United States Code, Section 1594 (Conspiracy to Commit Sex Trafficking), Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) and Title 18, United States Code, Section 2252 (Sexual Exploitation of Minors), including, for each account or identifier listed on Attachment A-2, information pertaining to the following matters, including attempting and conspiring to engage in the following matters:
 - a. Records relating to the purchase or placement of advertisements for commercial sex;
 - b. Records relating to the purchase or use of stored value cards, gift cards, and other financial instruments which may be used to purchase advertisements for commercial sex;
 - c. Records relating to the solicitation of customers for commercial sex;
 - d. Records relating to the scheduling of appointments for commercial sex;
 - e. Records relating to the travel or transportation of individuals to engage in commercial sex;
 - f. Records relating to sexually explicit or suggestive images of minors that may be used in furtherance of commercial sex trafficking;
 - g. Records relating to the recruitment, enticement, solicitation or coercion of individuals to engage in commercial sex;
 - h. Records relating to the fruits or instrumentalities of commercial sex trafficking, including currency and other financial instruments, jewelry, vehicles, controlled substances, and firearms.
2. Records relating to the kidnapping or attempts to escape from kidnapping of any individual.
3. Credit card and other financial information including but not limited to bills and payment records;
4. Evidence of who used, owned, or controlled the accounts or identifiers listed on Attachment A-2;

5. Evidence of the times the accounts or identifiers listed on Attachment A-2 were used;
6. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A-2 and other associated accounts.
7. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

III. By Order of the Court

Tagged shall disclose responsive data, if any, by sending it to Special Agent Patrick T. Winn, Federal Bureau of Investigation, electronically at ptwinn@fbi.gov, or by using the U.S. Postal Service or another courier service to 185 Admiral Cochrane Drive, Suite #101, Annapolis, MD, 21401.

ATTACHMENT A-3

DESCRIPTION OF LOCATION TO BE SEARCHED

(Facebook Account)

This warrant applies to information associated with the following Facebook account:

<https://www.facebook.com/ricky.rude.161>

that are stored at premises owned, maintained, controlled, or operated by Facebook Inc., a business headquartered at 1601 Willow Road, Menlo Park, California, 94025.

ATTACHMENT B-3
PARTICULAR THINGS TO BE SEIZED
(Facebook Account)

I. Files and Accounts to be produced by Facebook between 6/1/2017 – 1/10/2018

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Facebook including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Facebook or have been preserved pursuant to a preservation request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

a. Any and all associated subscriber information and user contact info, including, but not limited to, all “About Me” data, user identification number, current name and any prior names associated with the Target Account(s), alternate names, birth date, contact email addresses, including removed email addresses, physical addresses, associated or registered telephone numbers, associated screen names, associated websites, apps, registration date, and work data;

b. A user “neo-print,” including account status history, profile contact information, date and time of account creation, historical login information, mini-feed, status update history, shares, notes, wall and timeline postings to the Target Account(s), wall and timeline postings made by the Target Account(s) to other accounts, friend listing, including deleted or removed friends and friends identified as “Family,” the names of all users listed as “Followers” or as “Following,” networks, groups listing, future and past events, and video listing;

c. A user “photo-print,” including all undeleted or saved photos, photos in which the user has been “tagged” with the user name, and all associated metadata or EXIF data with any such photos;

d. Any and all associated Groups information, including a list of all other users currently registered in any such groups and the current status of the group profile;

e. Any and all public or private messages, including any attached documents, images, or photos, including from the Facebook Messenger app, the Facebook mobile app, and the Facebook website accessed via mobile device (including phone or tablet) or computer;

f. All notes written and published to the Target Account(s);

g. All Internet Protocol (“IP”) logs for the Target Account(s) from 6/1/2017 to the present, including script data, script get data, user ID, view time, IP source information, login and logout data, and active sessions data;

h. All chat history, including, but not limited to, the content of all chats and date and time information for all chats, including from the Facebook Messenger app, the Facebook mobile app, and the Facebook website accessed via mobile device (including phone or tablet) or computer;

i. All check-in data;

j. All Connections data, including, but not limited to, all users who have liked the Page or Place of the Target Account(s);

k. All stored credit card numbers;

l. All Events data;

m. All Friend Requests data, including pending sent and received friend requests;

n. All associated data that is "Hidden from News Feed," including any friends, apps, or pages hidden from the News Feed;

o. The last location associated with an update;

p. All "Likes on Other's Posts," "Likes on Your Posts from others," and "Likes on Other Sites" data;

q. A list of all linked accounts;

r. A list of all "Pages You Admin" for the accounts listed below;

s. All Physical Tokens data;

t. All Pokes data;

u. All Recent Activities data;

v. All Searches data;

w. All Shares data;

x. All videos posted to the Target Account(s);

y. The subscriber's registration information provided at time of account creation, including IP address(es);

z. The subscriber's service and account information, including any billing address(es) provided, billing records, telephone numbers, IP address (at each transaction), and complete transactional information;

aa. The subscriber's email address(es) and/or any email address(es) relating to the subscriber;

bb. The subscriber's records of session times and durations and any information relating to the session including, but not limited to, any temporarily assigned network address, Internet Protocol (IP) address, MAC address;

cc. The subscriber's length of service (including start date) and types of services utilized and any information associated with that service such Internet Protocol (IP) address, MAC address, Caller ID, and Automatic Number Identification (ANI);

dd. The subscriber's means and source of payment for any financial transactions (including any credit card or bank number);

ee. IP addresses and location data for all posts, wall posts, comments, friend requests, all messages and electronic communications, photo uploads, likes, Messenger messages and file transfers, and machine cookie information; and

ff. Interstitial Facebook, Facebook Messenger, and Instagram accounts linked to the Target Account(s) by usernames, e-mail addresses, SMS numbers, credit card numbers, bank account numbers.

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the account(s) described in Attachment A-3 which is evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1591 (Sex Trafficking of Children or By Force, Fraud, or Coercion), Title 18, United States Code, Section 1594 (Conspiracy to Commit Sex Trafficking), Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) and Title 18, United States Code, Section 2252 (Sexual Exploitation of Minors), specifically that relate to the following:

a. All records or other information relating to the recruitment, advertising, or operation of sex trafficking

b. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

c. Communication, information, documentation and records relating to who created, used, or communicated with the account(s) or identifier(s), including records about their identities and whereabouts;

d. Evidence of the times the account(s) or identifier(s) listed in Attachment A were used;

e. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

f. Passwords and encryption keys, and other access information that may be necessary to access the account(s) or identifier(s) and other associated accounts;

g. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account(s).

ATTACHMENT A-4

DESCRIPTION OF LOCATION TO BE SEARCHED

(Yahoo! / Oath Holding, Inc. Account)

This warrant applies to information associated with Oath Holdings, Inc. account:

ryandinero123@yahoo.com

which is stored at premises owned, maintained, controlled, or operated by Oath Holdings, Inc., a business with offices located at 701 First Avenue, Sunnyvale, California, 94089.

ATTACHMENT B-4

PARTICULAR THINGS TO BE SEIZED

(Yahoo! / Oath Holdings, Inc. Account)

I. Information to be disclosed

To the extent that the information described in Attachment A-4 is within the possession, custody, or control of [Oath Holdings, Inc.](#) (the “Target ISP”), the Target ISP is required to disclose the following information to the government for the accounts or identifiers listed in Attachment A (the “Target Account”). Such information should include the below-described content of the subject account:

- a. Subscriber Information, including the name and location, supplied by the user at the time of registration, the date the account was created and all of the services of the Target ISP used by each Target Account.
- b. Records of user activity for each connection made to or from the Target Accounts, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses, and any telephone, instrument or other unique identifiers collected by the Target ISP and associated with the Target Accounts;
- c. All information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);
- d. The contents of all e-mails stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- e. Any deleted emails, including any deleted information described in subparagraph “d,” above;
- f. All internet search records, including the specific terms searched in association with the Target Account, the dates, times and time zones of all searches, the IP addresses or

telephone or instrument identifying numbers associated with those searches, and any data related to the results of the searches associated with the Target Account and the Target Account's use of any search results;

- g. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of services utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- h. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, videos and other data files;
- i. All local and long distance telephone connection records;
- j. All telephone or instrument numbers associated with the Target Account (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"));
- k. All wire and electronic communications held or maintained by the Target ISP at any time in association with telephone communication services, including but not limited to text or SMS messaging and stored audio communications, for the use of or associated with the Target Account; and
- l. All records pertaining to communications between the Target ISP and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 1591 (Sex Trafficking of Children or By Force, Fraud, or Coercion), Title 18, United States Code, Section 1594 (Conspiracy to Commit Sex Trafficking), Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) and Title 18, United States Code, Section 2252 (Sexual Exploitation of Minors), including, for each account or identifier listed on Attachment A-4, information pertaining to the following matters, including attempting and conspiring to engage in the following matters:
 - a. Records relating to the purchase or placement of advertisements for commercial sex;
 - b. Records relating to the purchase or use of stored value cards, gift cards, and other financial instruments which may be used to purchase advertisements for commercial sex;
 - c. Records relating to the solicitation of customers for commercial sex;
 - d. Records relating to the scheduling of appointments for commercial sex;
 - e. Records relating to the travel or transportation of individuals to engage in commercial sex;
 - f. Records relating to sexually explicit or suggestive images of minors that may be used in furtherance of commercial sex trafficking;
 - g. Records relating to the recruitment, enticement, solicitation or coercion of individuals to engage in commercial sex;
 - h. Records relating to the fruits or instrumentalities of commercial sex trafficking, including currency and other financial instruments, jewelry, vehicles, controlled substances, and firearms.
2. Records relating to the kidnapping or attempts to escape from kidnapping of any individual.
3. Credit card and other financial information including but not limited to bills and payment records;

4. Evidence of who used, owned, or controlled the accounts or identifiers listed on Attachment A-4;
5. Evidence of the times the accounts or identifiers listed on Attachment A-4 were used;
6. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A-4 and other associated accounts.
7. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

III. By Order of the Court

Oath Holdings, Inc. shall disclose responsive data, if any, by sending it to Special Agent Patrick T. Winn, Federal Bureau of Investigation, electronically at ptwinn@fbi.gov or by using the U.S. Postal Service or another courier service to 185 Admiral Cochrane Drive, Suite #101 Annapolis, Maryland, 21401.